From Big Data To Cybersecurity, Today's Device-Makers Face Myriad Compliance Risks – But Being Proactive Can Pay Off, Ex-FDA Official Says

Too many medical device manufacturers are struggling because they don't have policies and systems in place to handle the ever-growing amount of data they receive about their products once they've gone to market.

As a result, important signals can go undetected or unaddressed, leading to compliance problems and devices that are of poor quality – both of which could ultimately affect a device-maker's bottom line. But Ricki Chase, a former US FDA investigations branch director, says firms can nip those troubles in the bud by being more proactive in their approach to tackling incoming quality data.

"Because the world has become so connected and everything has become so digitized, there's just an enormous amount of data out there for firms to collect," said Chase, now a compliance practice director for Lachman Consultant Services Inc. She joined Lachman in 2016 after spending 16 years at FDA, where she was also an investigator, medical device specialist and supervisory investigator.

"From data being shared on personal-use devices to medical devices being linked to a telemetry hub in a hospital setting, to devices that are speaking to doctors directly so they can monitor you remotely – the data is just incredible," Chase said. "But the problem with having that amount of data out there is, manufacturers aren't necessarily able to get their arms around it and understand what may be going on with their devices, and what may be impacting their performance."

Such an avalanche of data can throw a company's key performance indicators (KPIs) for a loop. KPIs are used to measure a company's success; for device-makers, one KPI might be how quickly they can send product to market, while another might gauge how devices are performing in the field.

For instance, "people go online and will say, 'I used this product and it burned me,' or 'This device shocked me.' That now becomes data that should be considered by a firm to be an event or complaint," Chase said. "But the problem is, a lot of times it's anecdotal information that's being collected. And there's a lot of it."

Because that type of data can be unreliable, a manufacturer can't be wholly sure that its KPI for complaint handling is accurate. "The sheer volume of data out there makes it really difficult for firms to keep their key performance indicators precise, timely and in line," she said.

Chase strongly urges companies to think more proactively by developing procedures to help them manage the increased regulatory risk posed by big data collection.

A lack of adequate policies to address the issue is "probably the No. 1 failure you see when device firms get into trouble with FDA, or end up having large market withdrawals or recalls," she said. "By nature, many people who work in a regulated area can be reactive rather than proactive. And when you're dealing with something like the large amount of data that's out there revolving around your device or your quality system, you must have systems designed and in place to be able to capture,

analyze and react to that data in a very timely way."

When those systems aren't proactively established, device-makers can have a difficult time keeping up with the data influx.

"Being reactive generally means that something bad has happened. And when nonconforming systems or products pop up, we all know that ends up costing a company much more in revenue than the initial capital investment of creating a proactive quality system," Chase said. "So, it's better to get it right the first time than to try to put a Band-Aid over it when something bad happens."

And when a company is proactive, it has already considered, for example, its many risk factors and conducted appropriate risk management activities on its devices. When firms do that, "and a problem does happen to show up post-market, those manufacturers are more readily able to respond to that in an appropriate way and solve that problem very quickly, as opposed to having to go back and scratch their head and wonder what went wrong," she said.

'Internet Of Things,' Cyber Threats Present Dangers To Compliance

Haphazardly handling big data is just one challenge to a manufacturer's efforts to be fully compliant with its many regulatory requirements. The so-called "Internet of Things" is also fast emerging as a compliance risk, and device firms need to be aware.

The Internet of Things – or IoT – is basically the ability for any item with a sensor to measure, analyze and send data to remote servers, and receive data in return, Chase explained.

"The Internet of Things includes consumer devices, such as my Apple Watch that 'talks' to my smartphone app," she said. "So, when I go to see my doctor, she will say, 'Have you been exercising?' and I say yes. And then she says, 'I don't believe you,' and I say, 'But wait, look, I can show you my workout log from my smartphone.' And if the doctor uses that to make a decision about my health – such as whether I should keep taking blood pressure medication – then that is a medical device function" and could be regulated.

That's because, FDA says, if a product produces data that can be shared with medical professionals to detect, cure, treat or mitigate a disease, then that product – even if it's a smartphone or a smartwatch – is a medical device and is thereby subject to scrutiny by regulators. (*See FD&C Act Sec. 321(h) (21 U.S.C. 321(h)*).

"So, it's not just a matter of manufacturers getting their arms around what's going on in the digital universe to control their KPIs, and understanding what's going on with their device or understanding where the market is being driven," Chase said. "Rather, it's also a situation where, because everything is interlinked via the Web, technology is producing new and challenging compliance considerations."

And cybersecurity is another concern, but not only because of the more obvious threats from malicious hackers who could, say, theoretically turn off pacemakers or overdose patients who use infusion pumps. As supply chains grow and become more complex, they too could fall prey to cyberattacks.

"It's not just our digital world that's becoming more complex, but our world in general is becoming more complex," Chase said. "Think about it: The supply chain is not like it used to be. The truck doesn't pull up with an invoice, and you sign the P.O. and the delivery slip, and you confirm you got what you ordered. Instead, suppliers use scanners and digital tablets, and they have digital tracking devices all along the supply chain. And everywhere that there is a digital interface, there's an opportunity for theft, there's an opportunity for counterfeiting, there's an opportunity for diversion.

"That just causes more trouble for the device-maker, who is ultimately responsible for ensuring the security of the entire supply chain and their product from cradle to grave."

Mergers And Acquisitions Also Pose Compliance Challenges

Meanwhile, manufacturers can further expose themselves to increased compliance risk when merging with or acquiring another device firm. That's because many companies wait until the last moment to conduct all-important due diligence activities and don't fully comprehend problems they might be unwittingly taking on.

"Quite frequently, what I experience is that a firm that wants to merge, or form a partnership, or acquire another firm, will bring in somebody to do a due diligence assessment very late in the game. Often, the due diligence is requested a mere five to 10 days before a business decision must be made about whether to move forward. That is a very short window of time in which to have somebody come in and do a due diligence assessment," Chase said.

She recommends that device-makers invest in due diligence activities early-on in the merger or acquisition process to prevent problems downstream.

"Just by the nature of doing business, due diligence isn't something that companies truly want to invest in," Chase said. "Instead, what they want to get is a very surface-level idea of, 'Do you think there are huge problems here, or are there minor problems?' And they ask frequently for people across varying industries to make those decisions or to give them advice on that, and then that's what they base a lot of their decision on – they just want to understand what type of risk they'll inherit."

Chase pointed out that the designs for devices made by the manufacturer being acquired are often overlooked during due diligence – a potentially fatal mistake.

"If you're purchasing a company, and by the purchase of that company you are buying or inheriting their 510(k) or their pre-market approval (PMA) for a device, you are probably hopeful that because the company has a 510(k) clearance or a PMA, that the device design is adequate," she said.

While PMAs from FDA typically guarantee good product design, 510(k)s can pose more significant dangers. "When it comes to a PMA, I would say the acquiring firm is probably very, very secure in understanding that the device design is there. Now, of course, whether the design has been maintained through

design control changes is another story," Chase said.

"But where firms can get in trouble is when they buy 510(k) devices, because the owner of the 510(k) only had to show substantial equivalence to gain access to the market. At no time did they have to submit that design to the FDA for review," she said. "And it's not until post-market inspection that you might find out that the design control either wasn't done originally, or it was done but it wasn't done well, or it was done but it's so old that all of the design changes that have occurred since then have not been incorporated anywhere."

After two manufacturers finally come together, the acquiring firm will typically fire the other company's top leaders, an action that Chase advises firms to handle with caution. "When that happens, now there are a bunch of people at the acquired firm that are the worker bees that are very unfamiliar with their new leaders, whom they're supposed to trust to lead them down the right path," she said. "Something like that can be a real culture shift for people, and can be extremely challenging."

The acquiring manufacturer also must decide how to best integrate quality systems, and to do it right.

"I've seen this happen frequently: You end up acquiring a company. You now have multiple sites. They all kind of do the same thing. Now they're all under one umbrella, but each of the locations is working under a different quality system – and they're all commonly owned," Chase said, noting that it can become "extremely complicated" for a firm in such a position to know what's happening systemically across its entire organization.

"And remember, at the end of the day the corporate entity is ultimately responsible for all of its sites. So, it can be very, very challenging to manage those locations when they're all so vastly different," she said.

A union between companies can also prove challenging when it comes to developing standard operating procedures and quality systems that are unique to the activities of specific facilities. "It's never one-size-fits-all," Chase said. "So, there's always going to be work to be done, whether you're trying to marry those quality systems, create a whole new quality system, or overcome the differences between the quality systems."

Investing In Quality Is Always A Wise Decision

In the end, device-makers can manage their many regulatory risks by having a robust, well-resourced strategy for compliance in place, as well as a healthy quality system.

"If you construct your quality system and your compliance strategy properly from the beginning, and you seriously invest and think about quality as an investment, then your firm will be more successful," Chase said. "It has been proven time and time again that investing in quality saves companies money in the long run. That's because being reactive to problems – particularly serious problems – costs firms tons of money in reputation, in product, in downtime and in diverted resources – resources that now must be used to remediate, not to mention having to hire a third-party to come into your facility and help you. It can be very, very expensive."

To catch the attention of top management, Chase suggests that quality and regulatory professionals place a dollar amount on the value of good, thorough quality.

"At most companies, quality is an afterthought, when it should be the first thought," she said. "It really starts with the management, and understanding that leadership comes from the top, and that they have to set the tone. If they set the tone that quality is first and foremost, and they create a system to be successful in that realm, then products do come to market faster. They generally come to market faster because a good quality system will identify problems early on and will help you correct problems the first time so you're not continually going back and fixing the same problems."

If using the persuasiveness of the purse strings doesn't work, those in quality and regulatory should make it personal for management.

"When I talk to senior leaders about investing in quality, I try to explain to them, or ask them, or converse with them: 'Why did you get into the industry in the first place? Why are you in the position you're in? What is your goal? And what do you think would make your company more profitable?' And then when they tell me what they think would make them be more profitable, I always try to link that back to a quality component, Chase said.

And if that still doesn't change top management's mind, then they should be reminded that their own job security is at stake if quality systems are poor.

The Bottom Line

"The medical device industry is growing very quickly. But it's not only growing quickly; it's becoming more and more technologically advanced, too. And because the technology is becoming so complex, there is increased risk to your devices and to your company with regard to your compliance," Chase said in summation.

"The expectation is that your firm will keep pace with industry developments and with the expectations for maintaining current good manufacturing practices," she said. "It's not just a matter of keeping pace and becoming more technologically advanced; it's also a matter of understanding what the different expectations are because of that, and what FDA's expectations are, and how you adjust – and how you can do that proactively, because being proactive reduces your compliance cost and can increase your bottom line."

Lachman CONSULTANTS